Fermat's Proof
of Fermat's Last Theorem

Johnny E. Magee

Abstract

Focusing on the properties and constraints of the decompositions of Fermat's equation and its elements —and employing only basic arithmetic and algebraic techniques that would have been known to Fermat— we identify certain specific requirements necessary for c, of $(a^n + b^n) = c^n$, to be an integer, and establish that these requirements can only be met at $n = 2$.

AMS Subject Classification (2010): Primary, 11D41
Key words and phrases: Fermat's Last Theorem, Fermat's Equation, Binomial Theorem

Contents

1 Introduction

The decomposition of mathematical objects (integers, variables, equations, expressions or their elements, vectors, etc.) is a tool used in virtually all of mathematics, from geometry and algebra and number theory to the teaching of elementary school math (decomposing 6,789 into 6 *thousands* + 7 *hundreds* + 8 *tens* + 9 *ones*).

While ‘decomposition‘ is generally characterized as the simplification or breaking down of a selected object into its constituent sub-components (e.g., 5 can be decomposed into $[(1+1)+(1+1+1)]$; 15 can be decomposed into $(3 \cdot 5)$), the critical usefulness of decomposition lies in the fact that it is always the *equivalent* restatement of a selected mathematical object, expressed in terms other than those of the original object.

Given the equation $(p+q) = r$, and the inverse operations $(r-p) = q$ and $(r-q) = p$; $(r-p)$ and $(r-q)$ can be viewed as decompositions (respectively) of q and p, and can be further utilized to arrive at an equivalent to, and thus a decomposition of, $(p+q)$ and r; $(p+q) = [(r-p)+(r-q)]$.

Such decompositions, particularly where they can be substituted in the original equation, or employed (or further decomposed and employed) in new equations, have the significant potential of revealing properties and constraints that might not otherwise be apparent, with any such properties and constraints inherent to the original object.

Pierre de Fermat’s margin note, 1637 [5, p. 139]:

> “It is impossible for a cube to be the sum of two cubes, a fourth power to be the sum of two fourth powers, or in general, for any number that is a power greater than the second to be the sum of two like powers.
> *I have discovered a truly marvelous demonstration of this proposition that this margin is too narrow to contain*” [7, p. 252][9].

FERMATS LAST THEOREM. For all $n > 2$, there are no solutions to the equation $(a^n + b^n) = c^n$ where a, b, c, n are all positive integers.

Let $c = \sqrt[n]{(a^n + b^n)}$. Let a, b, n be positive integers with (a,b) coprime and of opposite parity, $a < b < c$, and $n \geq 2$. A discussion of the ”why” of these constraints immediately follows.

If *a* and *b* are equal then $a^n = b^n$ and $(a^n + b^n) = (a^n + a^n) = 2a^n$, and

$$\sqrt[n]{(2a^n)} = (\sqrt[n]{2} \cdot \sqrt[n]{a^n}) = (\sqrt[n]{2} \cdot a).$$

Given that for all $n \geq 2$, n can be expressed in the form $n = (v \cdot w)$ where $v = 2$ and $w = (n/2)$, then $n = (2 \cdot (n/2))$, and $\sqrt[n]{2} = \sqrt[2 \cdot (n/2)]{2} = \sqrt[n/2]{\sqrt[2]{2}} = \sqrt[(n/2)]{\sqrt{2}}$;

and with the $\sqrt{2}$ an irrational non-integer [3, p. 20-21], and $\sqrt[(n/2)]{\sqrt{2}}$ the rational root of an irrational number, then the $\sqrt[n]{2}$ is irrational.

Demonstration

$$\begin{aligned}
\sqrt[2]{2} &= (\sqrt{2} = 1.41421356)\\
\sqrt[3]{2} &= 1.25992104 = \sqrt[(2\cdot(3/2))]{2} = \sqrt[(3/2)]{(\sqrt[2]{2})} = \sqrt[(3/2)]{(\sqrt{2})}\\
&= \sqrt[1.5]{1.41421356} = (\sqrt{1.41421356})^{(1/1.5)} = 1.25992104\\
\sqrt[4]{2} &= 1.18920711 = \sqrt[(2\cdot(4/2))]{2} = \sqrt[(4/2)]{(\sqrt[2]{2})} = \sqrt[(4/2)]{(\sqrt{2})}\\
&= \sqrt[2]{1.41421356} = (\sqrt{1.41421356})^{(1/2)} = 1.18920711\\
\sqrt[5]{2} &= 1.14869835 = \sqrt[(2\cdot(5/2))]{2} = \sqrt[(5/2)]{(\sqrt[2]{2})} = \sqrt[(5/2)]{(\sqrt{2})}\\
&= \sqrt[2.5]{1.41421356} = (\sqrt{1.41421356})^{(1/2.5)} = 1.14869835.\\
&\ldots
\end{aligned}$$

Then the $(\sqrt[n]{2} \cdot a)$, the product of an irrational number and an integer, is also irrational [2, p. 317], and $\sqrt[n]{(a^n + b^n)}$ being an integer is possible only if a and b are not equal.

If a and b are both odd then a can be restated in the form $(2x+1)$; b in the form $(2y+1)$; and c, an even integer, in the form $2z$, where x, y, z are all positive integers. Let the symbol "$\Rightarrow$" be read as "*then*". Let $n = 2$:

$$\begin{aligned}
(2z)^2 &= (2x+1)^2 + (2y+1)^2\\
4z^2 &= [(4x^2+4x+1)+(4y^2+4y+1)] \;=\; (4x^2+4x+4y^2+4y+2)\\
&\Rightarrow [4z^2 - (4x^2+4x+4y^2+4y)] = 2\\
2 &= [4 \cdot (z^2 - (x^2+x+y^2+y))].
\end{aligned}$$

Alternately, with 2 the greatest common divisor (GCD) of

$$[4z^2 = (4x^2+4x+4y^2+4y+2)],$$

then dividing both sides of our equation by 2 gives us

$$\begin{aligned}
2z^2 &= (2x^2+2x+2y^2+2y+1)\\
&= [(2 \cdot (x^2+x+y^2+y)) + 1].
\end{aligned}$$

The first of our alternate resolutions gives us that 2 is equal to $four$ times some other positive integer, which is impossible; while our second resolution makes the equally impossible declaration that an even integer is equal to an odd integer. In both cases, z is ultimately equal to the square root of a non-integer, giving us that where a and b are both odd, the square root of $(a^2 + b^2)$ can never be an integer.

If two integers share a common multiple, M, and are raised to the nth power, the integer M is irrelevant as to whether the nth root of their sum can be an integer.

Let a, b, n and $B.A.M.$ be positive integers with M common to B and A. Let $(B/M) = b$ and $(A/M) = a$. Then $(A^n + B^n) = [(M \cdot a)^n + (M \cdot b)^n]$, and

$$\begin{aligned}\sqrt[n]{(A^n + B^n)} &= \sqrt[n]{[(M \cdot a)^n + (M \cdot b)^n]} \\ &= \sqrt[n]{(M^n \cdot a^n) + (M^n \cdot b^n)} \\ &= \sqrt[n]{M^n} \cdot \sqrt[n]{(a^n + b^n)} \\ &= M \cdot \sqrt[n]{(a^n + b^n)}.\end{aligned}$$

And where A and B are both even and a product of $M-$ a power of 2; or M is an odd factor common to A and B, the $\sqrt[n]{(A^n + B^n)}$ will always resolve to a product of the integer M times the nth root of the sum of the coprime elements of A and B (a and b) raised to the nth power, and it is only the nth root of $(a^n + b^n)$ that determines if $\sqrt[n]{(A^n + B^n)}$ can be an intege and only such coprime values of a and b that we need consider in determining the veracity of Fermat's conjecture.

Then for all positive integers, a, b, c; where a and b are not equal, and a and b are not both odd, and a and b do not share a common multiple, one of a and b is always odd and the other even, with c always odd.

2 The Proof

Theorem 2.1 *For all $n > 2$ there are no solutions to the equation $(a^n + b^n) = c^n$ where a, b, c, n are all positive integers.*

Proof Given $(a^n + b^n) = c^n$ then $(c^n - a^n) = b^n$ and $(c^n - b^n) = a^n$. Since we have that for any c, a plus the difference between a and c, and b plus the difference between b and c, are both equal to c, then c can be restated in the form of a binomial, $c = (a + (c - a)) = (b + (c - b))$; with $(c^n - a^n) = [(a + (c - a))^n - a^n]$ and $(c^n - b^n) = [(b + (c - b))^n - b^n]$.

From the binomial theorem[1], we have that $(a + b)^n > ((a^n + b^n) = c^n) \Rightarrow [(a + b) > c,\ (c - a) < b,\ (c - b) < a]$:

$(a^n + b^n) > c^n \Rightarrow (a + b) > c$;

$$\begin{aligned}(a + b)^n &= a^n + c_1 a^{(n-1)} b^1 + c_2 a^{(n-2)} b^2 + c_3 a^{(n-3)} b^3 \\ &\quad + \cdots + c_{(n-1)} a^1 b^{(n-1)} + b^n \\ &= (a^n + b^n) + c_1 a^{(n-1)} b^1 + c_2 a^{(n-2)} b^2 + c_3 a^{(n-3)} b^3 \\ &\quad + \cdots + c_{(n-1)} a^1 b^{(n-1)},\end{aligned}$$

[1] First proven by the Persian mathematician, al Karaji (953 - 1029 A.D) [5, p. 77].

$(c-a) < b$;

$$\begin{aligned}(a+b) > c &\Rightarrow ((a+b)-1) > (c-1)\\ &\Rightarrow ((a+b)-2) > (c-2)\\ &\dots\\ &\Rightarrow [((a+b)-a) = b] > (c-a),\end{aligned}$$

$(c-b) < a$;

$$\begin{aligned}(a+b) > c &\Rightarrow ((a+b)-1) > (c-1)\\ &\Rightarrow ((a+b)-2) > (c-2)\\ &\dots\\ &\Rightarrow [((a+b)-b) = a] > (c-b).\end{aligned}$$

and that the second term of a binomial is a factor of every term of expansion except the leading term, giving us that for all $n \geq 2$, $(c^n - a^n)$ is a product of $(c-a)$ and $(c^n - b^n)$ is a product of $(c-b)$. Letting $(c^n - a^n)$ serve as our demonstration example:

Demonstration

$$\begin{aligned}(c^2-a^2) &= [(a+(c-a))^2 - a^2] \;=\; [a^2 + 2a(c-a) + (c-a)^2 - a^2]\\ &= [(a^2-a^2) + 2a(c-a) + (c-a)^2] \;=\; [2a(c-a) + (c-a)^2]\\ &= (c-a)\cdot[2a + (c-a)].\end{aligned}$$

$$\begin{aligned}(c^3-a^3) &= [(a+(c-a))^3 - a^3] \;=\; [a^3 + 3a^2(c-a) + 3a(c-a)^2 + (c-a)^3 - a^3]\\ &= [3a^2(c-a) + 3a(c-a)^2 + (c-a)^3]\\ &= (c-a)\cdot[3a^2 + 3a(c-a) + (c-a)^2]\end{aligned}$$

$$\begin{aligned}(c^5-a^5) &= [(a+(c-a))^5 - a^5]\\ &= [a^5 + 5a^4(c-a) + 10a^3(c-a)^2 + 10a^2(c-a)^3 + 5a(c-a)^4 + (c-a)^5 - a^5]\\ &= [5a^4(c-a) + 10a^3(c-a)^2 + 10a^2(c-a)^3 + 5a(c-a)^4 + (c-a)^5]\\ &= (c-a)\cdot[5a^4 + 10a^3(c-a) + 10a^2(c-a)^2 + 5a(c-a)^3 + (c-a)^4].\end{aligned}$$

$\dots$

With $(c^n - a^n) = ((a^n + b^n) - a^n) = b^n$ and $(c^n - b^n) = ((a^n + b^n) - b^n) = a^n$, and with 2 being the least value of n, then $(c-a)$ must divide b^2 and $(c-b)$ must divide $a^2 \dots$ and $(c-a)$ can be comprised only of distinct primes in b (and the integer '1' where b is odd), and $(c-b)$ can be comprised only of distinct primes in a (and the integer '1' where a is odd).

Then $(c-a)$ can only be an element of the set of the unique products of the distinct primes in b, less than b, of the same parity as b, that divides b^2; and $(c-b)$ can only be an element of the set of the unique products of the distinct primes in a, less than a, of the same parity as a, that divides a^2; with no power of any distinct prime in $(c-a)$ or in $(c-b)$ greater than its power in b^2 or a^2.

Let the symbol "$\in$" be read as *"in", "is contained in"*. Let P_a denote the qualifying set of the unique products of the distinct primes in a, and P_b the qualifying set of the unique products of the distinct primes in b. Let $n = 2$. Using the Pythagorean triple, (28,45,53), as an example, with $28 = (2^2 \cdot 7)$ and $45 = (3^2 \cdot 5)$, we have

$$P_a = \{2, 4, 8, 14, 16\}$$
$$P_b = \{1, 3, 5, 9, 15, 25, 27\},$$

and the possibility[2] of $c = \sqrt[n]{(a^n + b^n)}$ being an integer exists only if $(c-a) \in P_b$ and $(c-b) \in P_a$ such that $(a + (c - a)) = (b + (c - b))$:

$$[(a + (c - a)) = (b + (c - b))]$$
$$(28 + 25) = (45 + 8)$$
$$53 = 53.$$

Consider, given $(a^n + b^n) = c^n$, then

$[(a^n/\, b^n) + (b^n/\, b^n)] = (c^n/\, b^n)$	$[(b^n/\, a^n) + (a^n/\, a^n)] = (c^n/\, a^n)$
$[(a/b)^n + (b/b)^n] = (c/b)^n$	$[(b/a)^n + (a/a)^n] = (c/a)^n$
$[(a/b)^n + 1] = (c/b)^n;$	$[(b/a)^n + 1] = (c/a)^n;$

$$c^n = (a^n + b^n) \;=\; [b^n \cdot ((a/b)^n + 1)] \;=\; [a^n \cdot ((b/a)^n + 1)];$$
$$c = \sqrt[n]{c^n} \;=\; \sqrt[n]{(a^n + b^n))} \;=\; [b \cdot \sqrt[n]{((a/b)^n + 1)}] \;=\; [a \cdot \sqrt[n]{((b/a)^n + 1)}],$$

with the difference between c, and a and b, attributable to the amount by which the factors, $\sqrt[n]{((a/b)^n + 1)}$ and $\sqrt[n]{((b/a)^n + 1)}$, exceed $(b/b)^n = 1$ and $(a/a)^n = 1$:

$$(c - a) = [a \cdot (\sqrt[n]{((b/a)^n + 1)} - 1)];$$
$$(c - b) = [b \cdot (\sqrt[n]{((a/b)^n + 1)} - 1)].$$

Let the symbol "**N**" represent the set of positive whole numbers/integers. Then for any specified value of n, $c = \sqrt[n]{(a^n + b^n)}$ can be an integer, if and only if:

$[((a/b)^n + 1) = (c/b)^n]$ and $[((b/a)^n + 1) \;=\; (c/a)^n]$;

$(c - a) \in P_b$ and $(c - b) \in P_a$;

$((c - a) \in \mathbf{N}) = [a \cdot (\sqrt[n]{((b/a)^n + 1)} - 1)]$ and $((c - b) \in \mathbf{N}) = [b \cdot (\sqrt[n]{((a/b)^n + 1)} - 1)]$;

$$c = [(a + (c - a)) \;=\; (b + (c - b))] \;=\; [b \cdot \sqrt[n]{((a/b)^n + 1)}] \;=\; [a \cdot \sqrt[n]{((b/a)^n + 1)}];$$
$$c^n = [(b^n \cdot ((a/b)^n + 1)) \;=\; (b^n \cdot (c/b)^n)] \;=\; [(a^n \cdot ((b/a)^n + 1)) \;=\; (a^n \cdot (c/a)^n)].$$

[2] $(a+(c-a)) = (b+(c-b))$ holds for all $(c > b)$ and multiple complementary $(c-a)$,$(c-b)$ values may exist in P_b, P_a— though with $(c - a) = [a \cdot (\sqrt[n]{((b/a)^n + 1)} - 1)]$ and $(c - b) = [b \cdot (\sqrt[n]{((a/b)^n + 1)} - 1)]$ in **N**, only one matching $(c-a)$ and $(c-b)$ value can exist in P_b, P_a.

Demonstration

Let $n = 2$:

$$
\begin{aligned}
((a/b)^2 + 1) &= (c/b)^2 \\
((28/45)^2 + 1) &= (53/45)^2 \\
(0.62222222^2 + 1) &= 1.17777777^2 \\
(0.38716049 + 1) &= 1.38716049 \\
1.38716049 &= 1.38716049.
\end{aligned}
$$

$$
\begin{aligned}
c &= [b \cdot \sqrt{((a/b)^2 + 1)}] \\
&= [45 \cdot \sqrt{((28/45)^2 + 1)}] \;=\; [45 \cdot \sqrt{(0.62222222^2 + 1)}] \\
&= [45 \cdot \sqrt{(0.38716049 + 1)}] \;=\; (45 \cdot \sqrt{1.38716049}) \\
&= (45 \cdot 1.17777777). \\
&= 53
\end{aligned}
$$

$$
\begin{aligned}
c^2 &= [b^2 \cdot ((a/b)^2 + 1)] \;=\; [45^2 \cdot ((28/45)^2 + 1)] \\
&= \;[45^2 \cdot (0.62222222^2 + 1)] \;=\; [45^2 \cdot (0.38716049 + 1)] \\
&= \;(2025 \cdot 1.38716049) \;=\; 2809. \\
&= 53^2
\end{aligned}
$$

and

$$
\begin{aligned}
(c - a) &= [a \cdot (\sqrt[n]{((b/a)^2 + 1)} - 1)] \;=\; [28 \cdot (\sqrt{((45/28)^2 + 1)} - 1)] \\
&= [28 \cdot (\sqrt{(1.60714285^2 + 1)} - 1)] \;=\; [28 \cdot (\sqrt{(2.58290816 + 1)} - 1)] \\
&= [28 \cdot (\sqrt{(3.58290816)} - 1)] \;=\; [28 \cdot (1.89285714 - 1)] \\
&= (28 \cdot 0.89285714). \\
&= 25
\end{aligned}
$$

$$
\begin{aligned}
(c - b) &= [b \cdot (\sqrt[n]{((a/b)^2 + 1)} - 1)] \;=\; [45 \cdot (\sqrt{((28/45)^2 + 1)} - 1)] \\
&= [45 \cdot (\sqrt{(0.62222222^2 + 1)} - 1)] \;=\; [45 \cdot (\sqrt{(0.38716049 + 1)} - 1)] \\
&= [45 \cdot (\sqrt{(1.38716049)} - 1)] \;=\; [45 \cdot (1.17777777 - 1)] \\
&= (45 \cdot 0.17777777). \\
&= 8.
\end{aligned}
$$

While $(c - a) = [a \cdot (\sqrt[n]{((b/a)^n + 1)} - 1)]$ and $(c - b) = [b \cdot (\sqrt[n]{((a/b)^n + 1)} - 1)]$ will always give us the complements to a and b, yielding c for any value of n,

$$
\begin{aligned}
c &= \sqrt[3]{(a^3 + b^3)} \;=\; \sqrt[3]{(28^3 + 45^3)} \;=\; \sqrt[3]{(21952 + 91125)} \;=\; \sqrt[3]{113077} \\
&= 48.35685999;
\end{aligned}
$$

$$
(c - a) = (48.35685999 - 28) \;=\; 20.35685999;
$$

$$
\begin{aligned}
(c - a) &= [a \cdot (\sqrt[n]{((b/a)^n + 1)} - 1)] \;=\; [28 \cdot (\sqrt[3]{((45/28)^3 + 1)} - 1)] \\
&= [28 \cdot (\sqrt[3]{(1.60714285^3 + 1)} - 1)] \;=\; [28 \cdot (\sqrt[3]{(4.15110240 + 1)} - 1)] \\
&= [28 \cdot (\sqrt[3]{5.15110240} - 1)] \;=\; [28 \cdot (1.72703071 - 1)] \;=\; (28 \cdot 0.72703071) \\
&= 20.35685999,
\end{aligned}
$$

where $c = \sqrt[n]{(a^n + b^n)}$ is an integer, then $(c-a)$ and $(c-b)$ are also integers and $(c-a)$ must divide $(c^2-a^2) = ((a^2+b^2)-a^2) = b^2$, and $(c-b)$ must divide $(c^2-b^2) = ((a^2+b^2)-b^2) = a^2$;

• And with $(c-a)$, the divisor of b^2, equal to $[a \cdot (\sqrt{((b/a)^2+1)} - 1)]$, and $(c-b)$ the divisor of a^2, equal to $[b \cdot (\sqrt{((a/b)^2+1)} - 1)]$, with $(c-a) \in P_b$ and $(c-b) \in P_a$;

• And their being no possibility that for any $n > 2$, $[a \cdot (\sqrt[n]{((b/a)^n+1)} - 1)]$ can equal $[a \cdot (\sqrt{((b/a)^2+1)} - 1)]$, or that $[b \cdot (\sqrt[n]{((a/b)^n+1)} - 1)]$ can equal $[b \cdot (\sqrt{((a/b)^2+1)} - 1)]$,

• Then there can exist no other values of $(c-a)$ and $(c-b)$ that will divide all b^n and a^n, and $c = \sqrt[n]{(a^n+b^n)}$ can be an integer only where $n = 2$ and $(c-a) \in P_b$ and $(c-b) \in P_a$, and $c = a + [(c-a) = (a \cdot (\sqrt{((b/a)^2+1)} - 1))] = b + [(c-b) = (b \cdot (\sqrt{((a/b)^2+1)} - 1))]$.

Further, where $c = \sqrt{(a^2+b^2)}$ is an integer, the increase in the magnitude of $(c/b)^2$ above that of $(b/b)^2$ is equal to $(a/b)^2$; and with $a < b < c$, $(a/b) < 1$ and[3] $(c/b) > 1 < \sqrt{2}$; as n increases beyond 2, the magnitude of $(a/b)^n$ continually decreases while the magnitude of $(c/b)^n$ continually increases, such that for all $n > 2$, $((a/b)^n+1) < (c/b)^n \ldots$ and $[b^n \cdot ((a/b)^n+1)]$ can never equal $[b^n \cdot (c/b)^n]$.

Let the symbol "$\stackrel{?}{=}$" serve to indicate that the actual equality of the left-hand-side and right-hand-side of the immediately following equations are indeterminable until we arrive at their final resolution. Continuing with $(a,b) = (28, 45)$:

Demonstration

Let $n = 2$;

$$((a^n/b^n) + (b^n/b^n)) \stackrel{?}{=} ((a + (c-a)) \;/\; b)^n$$
$$[(a/b)^n + 1] \stackrel{?}{=} ((28+25) \;/\; 45)^n$$
$$[(28/45)^2 + 1] \stackrel{?}{=} (53/45)^2$$
$$(0.62222222^2 + 1) \stackrel{?}{=} 1.17777777^2$$
$$(0.38716049 + 1) \stackrel{?}{=} 1.17777777^2$$
$$1.38716049 = 1.38716049.$$

Let $n = 3$;

$$[(a/b)^n + 1] \stackrel{?}{=} ((28+25) \;/\; 45)^n$$
$$[(28/45)^3 + 1] \stackrel{?}{=} (53/45)^3$$
$$(0.62222222^3 + 1) \stackrel{?}{=} 1.17777777^3$$
$$(0.24089986 + 1) \stackrel{?}{=} 1.17777777^3$$
$$1.24089986 \neq 1.63376680.$$

[3] If $(c/b) > \sqrt{2}$ then $(c/b)^n > 2$, $c > (a+b)$, and $c^n > 2b^n > (a^n + b^n)$.

Let $n = 4$;

$$[(a/b)^n + 1] \stackrel{?}{=} ((28 + 25)\ /\ 45)^n$$
$$[(28/45)^4 + 1] \stackrel{?}{=} (53/45)^4$$
$$(0.62222222^4 + 1) \stackrel{?}{=} 1.17777777^4$$
$$(0.14989324 + 1) \stackrel{?}{=} 1.17777777^4$$
$$1.14989324 \neq 1.92421423.$$

And this I believe was Fermat's "*truly marvelous*" discovery:

That where c is an integer, and thus $(c - a)$ and $(c - b)$, they are all defined for all values of n at $n = 2$; that $c = \sqrt[n]{(a^n + b^n)}$ can be an integer, if and only if $[(a/b)^n + 1] = (c/b)^n$; and that it is only at $n = 2$ that such an equality between $[(a/b)^n + 1]$ and $(c/b)^n$ can occur... giving us that $\sqrt[n]{(a^n + b^n)}$ can be an integer only at $n = 2$, and that for all $n > 2$ there are no positive integers a, b, c, n such that $(a^n + b^n) = c^n$. ■

3 The Proof – Further Implications

Remark Paulo Ribenboim in "Lecture One" of his book, *13 Lectures on Fermat's Last Theorem* (1979), and Thomas Koshy in *Elementary Number Theory With Applications*, point out the fact that since every integer $n > 2$ is a product of 4 or of an odd prime [8, p. 2], then with Fermat (and others) having proved the case for $n = 4$ [8, p. 2][1, p. 44], all that is required to complete the proof of Fermat's conjecture is to prove that it holds true for all odd primes [8, p. 3][6, p. 546].

Proposition 3.1 *For all odd $n > 2$, encompassing the set of all odd primes, $(a^n + b^n)$ is a product of $(a + b)$ and $\sqrt[n]{(a^n + b^n)}$ can never be an integer.*

Proof Per the binomial theorem the expansion of $(a + b)^n$ proceeds according to the form [4, p. 550],

$$(a + b)^n = c_0 a^n b^0 + c_1 a^{(n-1)} b^1 + c_2 a^{(n-2)} b^2 + c_3 a^{(n-3)} b^3 + \dots + c_{(n-1)} a^1 b^{(n-1)} + c_n a^0 b^n,$$

where c_0 through c_n are the integer coefficients of the successive terms of expansion, with c_0 and c_n equal to 1, c_1 and $c_{(n-1)}$ equal to n, and c_1 through c_n determinable by simple calculation.

The expansion generates a total of $(n + 1)$ terms where the sum of the exponents of a and b in each term is equal to n; with the second term of our binomial a factor of every term of expansion except the leading term such that if we exclude the leading term, each of the remaining terms (and their sum) is a product of the second term of our binomial.

Where $n > 2$ is odd, the expansion of $(a+b)^n$ consists of two groups of $(n+1)/2$ terms where the integer coefficients of the first $(n+1)/2$ terms repeat in the subsequent $(n+1)/2$ terms, with the exponents of a and b in the coefficient corresponding terms of the second group the reverse of those in the first group.

If we reassociate the terms of our expansion by integer coefficient, each of our reassociated pairs can be reduced to a product of our coefficient and the least exponent power of a and b within that pair, times the sum of equal powers of a and b; with the matching exponents of a and b equal to the greatest exponent within our pair minus the least exponent. The sequence of reassociated pairs of $(a+b)^n$ are then of the form,

$$\begin{aligned}(a+b)^n = {} & [c_0(a^n+b^n) + c_1 ab(a^{(n-2)} + b^{(n-2)}) + c_2 a^2b^2(a^{(n-4)} + b^{(n-4)}) \\ & + c_3a^3b^3(a^{(n-6)} + b^{(n-6)}) + \cdots + c_{(n-1)/2}(a^{(n-1)/2} \cdot b^{(n-1)/2}(a+b)].\end{aligned}$$

With n an odd integer, the exponents $(n-2), (n-4), (n-6), \ \ldots, (n-(n-1))$ are all odd and each of our reduced reassociated pairs is the product of the sum of the successively declining odd exponent powers of a and b from n to 1, such that $(a+b)^n$ is the sum of the products of

$$(a^n+b^n),\ (a^{(n-2)}+b^{(n-2)}),\ (a^{(n-4)}+b^{(n-4)}),\ \ldots,\ (a^1+b^1).$$

Demonstration

$$\begin{aligned}(a+b)^3 &= [a^3+3a^2b+3ab^2+b^3] \\ &= [(a^3+b^3)+(3a^2b+3ab^2)] \\ &= [(a^3+b^3)+3ab(a^1+b^1)].\end{aligned}$$

$$\begin{aligned}(a+b)^5 &= (a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5) \\ &= [(a^5+b^5)+(5a^4b+5ab^4)+(10a^3b^2+10a^2b^3)] \\ &= [(a^5+b^5)+5ab(a^3+b^3)+10a^2b^2(a^1+b^1)].\end{aligned}$$

$$\begin{aligned}(a+b)^7 &= (a^7+7a^6b+21a^5b^2+35a^4b^3+35a^3b^4+21a^2b^5+7ab^6+b^7) \\ &= [(a^7+b^7)+(7a^6b+7ab^6)+(21a^5b^2+21a^2b^5)+(35a^4b^3+35a^3b^4)] \\ &= [(a^7+b^7)+7ab(a^5+b^5)+21a^2b^2(a^3+b^3)+35a^3b^3(a^1+b^1)].\end{aligned}$$

$$\begin{aligned}(a+b)^9 &= (a^9+9a^8b+36^a7b^2+84a^6b^3+126a^5b^4+126a^4b^5+84a^3b^6+36a^2b^7 \\ &\quad +9ab^8+b^9) \\ &= [(a^9+b^9)+(9a^8b+9ab^8)+(36a^7b^2+36a^2b^7)+(84a^6b^3+84a^3b^6) \\ &\quad +(126a^5b^4+126a^4b^5)] \\ &= [(a^9+b^9)+9ab(a^7+b^7)+36a^2b^2(a^5+b^5)+84a^3b^3(a^3+b^3) \\ &\quad +126a^4b^4(a^1+b^1)].\end{aligned}$$

Then (a^n+b^n) is equal to $(a+b)^n$, minus our reduced reassociated inside terms—and for each successive increase in our odd n exponent, we are able to replace each lesser exponent sum of powers of $(a+b)$ with its equivalent reduction to a product of $(a+b)$; and, given $(a+b)^n = [(a+b)(a+b)^{(n-1)}]$, reduce (a^n+b^n) to a product of $(a+b)$:

$$
\begin{aligned}
(a+b)^3 &= (a^3 + 3a^2b + 3ab^2 + b^3)\\
&= (a^3+b^3) + (3a^2b + 3ab^2)\\
&= [(a^3+b^3) + 3ab(a+b)]\\
&\Rightarrow\\
(a^3+b^3) &= [(a+b)^3 - 3ab(a+b)]\\
&= [(a+b)(a+b)^2 - 3ab(a+b)]\\
&= (a+b)\cdot[(a+b)^2 - 3ab].
\end{aligned}
$$

$$
\begin{aligned}
(a+b)^5 &= (a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5)\\
&= [(a^5+b^5) + 5ab(a^3+b^3) + 10a^2b^2(a^1+b^1)]\\
&\Rightarrow\\
(a^5+b^5) &= (a+b)^5 - [5ab(a^3+b^3) + 10a^2b^2(a+b)]\\
&\textbf{Replace } (\boldsymbol{a^3+b^3}) \textbf{ with equivalent product of } (\boldsymbol{a+b})\textbf{:}\\
&= (a+b)^5 - [5ab((a+b)\cdot((a+b)^2 - 3ab)) + 10a^2b^2(a+b)]\\
&= (a+b)(a+b)^4 - [(a+b)\cdot(5ab(((a+b)^2 - 3ab)) + 10a^2b^2)]\\
&= (a+b)\cdot[(a+b)^4 - (5ab(((a+b)^2 - 3ab)) + 10a^2b^2)]\\
&= (a+b)\cdot[(a+b)^4 - (5ab(a+b)^2 - 15a^2b^2 + 10a^2b^2)]\\
&= (a+b)\cdot[(a+b)^4 - (5ab(a+b)^2 - 5a^2b^2)]\\
&= (a+b)\cdot[(a+b)^4 - (5ab((a+b)^2 - ab))].
\end{aligned}
$$

With the final term of (a^n+b^n) always a product of $(a+b)$, and (a^5+b^5) and (a^3+b^3) products of $(a+b)$, then (a^7+b^7) is reducible to a product of $(a+b)$;

$$(a^7+b^7) = (a+b)^7 - [7ab(a^5+b^5) + 21a^2b^2(a^3+b^3) + 35a^3b^3(a+b)],$$

and with (a^7+b^7), (a^5+b^5) and (a^3+b^3) all products of $(a+b)$, then (a^9+b^9) is a product of $(a+b)$;

$$
\begin{aligned}
(a^9+b^9) = (a+b)^9 - [&9ab(a^7+b^7) + 36a^2b^2(a^5+b^5) + 84a^3b^3(a^3+b^3)\\
&+ 126a^4b^4(a+b))],
\end{aligned}
$$

then $(a^{11}+b^{11})$ is a product of $(a+b)$...

$$
\begin{aligned}
(a^{11}+b^{11}) = (a+b)^{11} - [&11ab(a^9+b^9) + 55a^2b^2(a^7+b^7)\\
&+ 165a^3b^3(a^5+b^5) + 330a^4b^4(a^3+b^3) + 462a^5b^5(a+b)]
\end{aligned}
$$

...

and our operations repeat with each increase in n, giving us that for all odd $n > 2$, $(a^n + b^n)$ is a product of $(a + b)$.

With $a < b < c$ and $(a + b) > c$ then $c = \sqrt[n]{(a^n + b^n)}$ can be an integer only if $c \in \{(b+1), (b+2), (b+3), \ldots, ((b+a)-1))\}$ and $c = [(a+(c-a)) = (b+(c-b))]$; with $((c-a) = [a \cdot (\sqrt{((b/a)^2 + 1)} - 1)]) \in P_b$ and $((c-b) = [b \cdot (\sqrt{((a/b)^2 + 1)} - 1)]) \in P_a$.

But it can never happen. For we have that $(a + b)$, the divisor of all odd n, $(a^n + b^n)$, can be restated in the form,

$$(a + b) = [(a + (c - a)) + (b - (c - a))].$$

And with the integer c equal to $(a + (c - a))$ and b coprime to c; and $(c - a) < b$ comprised only of distinct primes in b, then $(b - (c - a))$ will contain prime(s) in b, coprime to c; and $(a+b) = [c+(b-(c-a))]$, will always contain primes not in c.

Then $(a + b)$, the divisor of all odd n, $(a^n + b^n)$, can never be a divisor of $c^n = [(a + (c - a))^n = (b + (c - b))^n] \ldots$ and for all odd n (encompassing the set of all odd primes), $(a^n + b^n)$ can never equal $[(a + (c - a))^n = (b + (c - b))^n]$ and $\sqrt[n]{(a^n + b^n)}$ can never be an integer. ■

Proposition 3.2 *For all odd $n > 2$, encompassing the set of all odd primes, $c = \sqrt[n]{(a^n + b^n)}$ can never be an integer.*

Proof Where $c = \sqrt[n]{(a^n + b^n)}$ is an integer then c is odd and a and b are of opposite parity and one of $(c - a)$ and $(c - b)$ is also odd and the other even. Let $(c - a)$ be the even quantity of $(c - a)$ and $(c - b)$ (Note: The results would be the same if we let $(c - b)$ be the even quantity). With $(c - a)$ a factor of every term of $(c^n - a^n)$,

$$\begin{aligned}(c^n - a^n) &= [(a + (c - a))^n - a^n] \\ &= na^{(n-1)}(c - a) + c_2a^{(n-2)}(c - a)^2 + c_3a^{(n-3)}(c - a)^3 + \ldots \\ &\quad + c_{(n-2)}a^{(n-(n-2))}(c - a)^{(n-2)} + na^{(n-(n-1))}(c - a)^{(n-1)} + c_n(c - a)^n,\end{aligned}$$

and the exponents of $(c - a)$ beginning at 1 and incrementing to n, then $(c^n - a^n) = [(a + (c - a))^n - a^n]$ is further reducible to the form,

$$\begin{aligned}(c^n - a^n) = (c - a) \cdot [na^{(n-1)} + (c - a) \cdot (c_2a^{(n-2)} + (c - a) \cdot (c_3a^{(n-3)} \\ + \cdots + (c - a) \cdot (c_{(n-2)}a^{(n-(n-2))} + (c - a) \cdot (na + (c - a)))))],\end{aligned}$$

Demonstration

$$\begin{aligned}(c^2 - a^2) &= [(a + (c - a))^2 - a^2] \\ &= [a^2 + 2a(c - a) + (c - a)^2 - a^2] \\ &= [2a(c - a) + (c - a)^2)] \\ &= (c - a) \cdot [2a + (c - a)].\end{aligned}$$

$$
\begin{aligned}
(c^3 - a^3) &= [3a^2(c-a) + 3a(c-a)^2 + (c-a)^3] \\
&= (c-a) \cdot [3a^2 + 3a(c-a) + (c-a)^2] \\
&= (c-a) \cdot [3a^2 + (c-a)(3a + (c-a))] \\
(c^4 - a^4) &= (c-a) \cdot [4a^3 + 6a^2(c-a) + 4a(c-a)^2 + (c-a)^3] \\
&= (c-a) \cdot [4a^3 + (c-a)(6a^2 + 4a(c-a) + (c-a)^2)] \\
&= (c-a) \cdot [4a^3 + (c-a)(6a^2 + (c-a)(4a + (c-a)))] \\
(c^5 - a^5) &= [(c-a) \cdot [5a^4 + 10a^3(c-a) + 10a^2(c-a)^2 + 5a(c-a)^3 + (c-a)^4] \\
&= (c-a) \cdot [5a^4 + (c-a)(10a^3 + 10a^2(c-a) + 5a(c-a)^2 + (c-a)^3)] \\
&= (c-a) \cdot [5a^4 + (c-a)(10a^3 + (c-a)(10a^2 + 5a(c-a) + (c-a)^2))] \\
&= (c-a) \cdot [5a^4 + (c-a)(10a^3 + (c-a)(10a^2 + (c-a)(5a + (c-a))))] \\
\ldots
\end{aligned}
$$

And with the further reduction pattern the same for all $(c^n - a^n)$,

$$
\begin{aligned}
(c^2 - a^2) &= (c-a) \cdot [na^{(n-1)} + (c-a)] \\
(c^3 - a^3) &= (c-a) \cdot [na^{(n-1)} + (c-a) \cdot (na + (c-a))] \\
(c^4 - a^4) &= (c-a) \cdot [na^{(n-1)} + (c-a) \cdot (6a^2 + (c-a) \cdot (na + (c-a)))] \\
(c^5 - a^5) &= (c-a) \cdot [na^{(n-1)} + (c-a) \cdot (10a^3 + (c-a) \cdot (10a^2 \\
&\qquad + (c-a) \cdot (na + (c-a))))],
\end{aligned}
$$

and with 2 the least value of n, then $(c-a)$ must divide b^n at $n = 2$ and no power of any distinct prime in $(c-a)$ can be greater than its power in b^2.

Then with $(c-a)$ a product of 2 and the power of 2 in $(c-a)$ never greater than the square of the power of 2 in b; and for all $n > 2$, the power of 2 in b^n equal to the power of 2 in b raised to the nth power; then the possibility that $(c^n - a^n) = b^n$ only exists if the power of 2 in $(c^n - a^n)$ can be elevated to a power greater than that in $(c-a)$. Let $n > 2$ be odd.

Analyzing the sequence of operations, from right-to-left (RTL), within the further-reduced bracketed co-factor of $(c-a)$, we have an initial rightmost operation of $(na + (c-a))$.

With a coprime to $(c-a)$ and a and n odd, $(na + (c-a))$ is odd and void of any factors of 2.

Our next operation (stepping to the left) is the multiplication of our initial operation result by $(c-a)$, giving us a product of $(c-a)$; to which we then add the product of a power of a and it's coefficient.

As previously, with a coprime to $(c-a)$, our sum can contain a factor of 2 only if the coefficient of a is also a product of 2.

And this multiplication-then-addition process continually repeats until we arrive at the final operation within our bracketed co-factor of $(c-a)$, the sum of $na^{(n-1)}$ plus a product of $(c-a)$.

Again, with a and n odd and a coprime to $(c-a)$, $na^{(n-1)}$ plus a product of $(c-a)$ is odd and void of any factors of 2… and $(c^n - a^n) = [(a+(c-a))^n - a^n]$ is the product of a unique and distinct factor of $(c-a)$, with the power of 2 in $(c-a)$, and thus in $(c^n - a^n)$, never greater than the power of 2 in b^2.
Let $(a, b, c) = (5, 12, 13)$.

Demonstration

$$
\begin{aligned}
(c^2 - a^2) &= [(c-a)(c+a)] \\
&= [(13-5)(13+5)] = (8 \cdot 18) = (\mathbf{2^3} \cdot (2 \cdot 3^2)) \\
(c^3 - a^3) &= (13^3 - 5^3) = [(2197 - 125) = 2072] = (\mathbf{2^3} \cdot 259) \\
(c^5 - a^5) &= (13^5 - 5^5) = [(371293 - 3125) = 368168] = (\mathbf{2^3} \cdot 46021) \\
(c^7 - a^7) &= (13^7 - 5^7) = [(62748517 - 78125) = 62670392] = (\mathbf{2^3} \cdot 7833799) \\
&\ldots
\end{aligned}
$$

Then for all odd $n > 2$, encompassing the set of all odd primes, the power of 2 in $(c^n - a^n)$ can never equal the power of 2 in b^n, $(c^n - a^n)$ can never equal b^n, and $c = \sqrt[n]{(a^n + b^n)}$ can never be an integer. ■

Proposition 3.3 *Where $n > 2$ is equal to a power of 2 and $(c-a)$ is even, $c = \sqrt[n]{(a^n + b^n)}$ can never be an integer*

Proof Let $n > 2$ be a power of 2. Given $(a^n + b^n) = c^n$ then $(c^n - a^n) = b^n$ and $(c^n - b^n) = a^n$. Let $(c^n - a^n)$ be the even quantity of $(c^n - a^n)$ and $(c^n - b^n)$.

With $n > 2$ equal to a power of 2 then $(c^n - a^n)$ can be restated as a difference of squares of exponent $n/2$, $(c^n - a^n) = [(c^{n/2} - a^{n/2})(c^{n/2} + a^{n/2})]$, with each resulting, greater than 2, even-exponent-quotient difference of powers further reducible to a sum and difference of squares, such that $(c^n - a^n)$ is ultimately a product of $(c^2 - a^2) = (c-a)(c+a)$, times the *sums of powers* of c and a of exponents 2 to $n/2$. Let $n = (2^4 = 16)$. Then

Demonstration

$$
\begin{aligned}
(c^{16} - a^{16}) &= [(c^8)^2 - (a^8)^2] \;=\; [(c^8 - a^8)(c^8 + a^8)] \;=\; [((c^4)^2 - (a^4)^2) \cdot (c^8 + a^8)] \\
&= [(c^4 - a^4)(c^4 + a^4)(c^8 + a^8)] \;=\; [((c^2)^2 - (a^2)^2) \cdot (c^4 + a^4)(c^8 + a^8)] \\
&= [(c^2 - a^2)(c^2 + a^2)(c^4 + a^4)(c^8 + a^8)] \\
&= [(c-a)(c+a) \cdot (c^2 + a^2)(c^4 + a^4)(c^8 + a^8)].
\end{aligned}
$$

With $(c^n - a^n)$ even and $(c^2 - a^2) = (c-a)(c+a)$, and with 2 common to $(c-a)$ and $(c+a)$, then

$$
\begin{aligned}
(c+a) &= ((c-a) + 2a) \\
&= [2 \cdot ((c-a)/2 + a)].
\end{aligned}
$$

And with a odd and coprime to $(c-a)$, no odd integer in $(c-a)$ can exist in $(c+a)$. Then if the power of 2 in $(c-a)$ is equal to 2^1, $(c-a)/2$ is odd and $((c-a)/2+a)]$ is even; *and the power of 2 in* $(c+a) = [2\cdot((c-a)/2+a)]$ *is greater than* 2^1.

If the power of 2 in $(c-a)$ is greater than 2^1 then $(c-a)/2$ remains even and $((c-a)/2+a)]$ is odd, and the power of 2 in $(c+a) = [2\cdot((c-a)/2+a)]$ is equal to 2^1.

Then for all $n \geq 2$, one of $(c-a)$ and $(c+a)$ is always a product of 2^1 and the other a product of 2^2 or greater.

Similarly, just as $(c+a) = ((c-a)+2a)$, $(c^2+a^2) = ((c^2-a^2)+2a^2)$, and with a odd and 2 also common to (c^2-a^2), then

$$(c^2+a^2) = ((c^2-a^2)+2a^2) \; = \; [2\cdot((c-a)(c+a)/2+a^2)],$$

and with $(c-a)$ and $(c+a)$ even, $(c-a)(c+a)/2$ remains a product of 2 and $((c-a)(c+a)/2+a^2)$ is odd, and $[2\cdot((c-a)(c+a)/2+a^2)]$ is a product of the unique factor, 2^1. Likewise:

$$\begin{aligned}(c^4+a^4) = ((c^4-a^4)+2a^4) \; &= \; [(c-a)(c+a)(c^2+a^2)+2a^4] \\ &= [2\cdot((c-a)(c+a)(c^2+a^2)/2+a^4)],\end{aligned}$$

and with $((c-a)(c+a)(c^2+a^2)/2)$ even, $[((c-a)(c+a)(c^2+a^2)/2)+a^4]$ is odd, and $[2\cdot((c-a)(c+a)(c^2+a^2)/2+a^4)]$ is a product of 2^1. Continuing:

$$\begin{aligned}(c^8+a^8) = ((c^8-a^8)+2a^8) \; &= \; [(c-a)(c+a)(c^2+a^2)(c^4+a^4)+2a^8] \\ &= [2\cdot((c-a)(c+a)(c^2+a^2)(c^4+a^4)/2+a^8)],\end{aligned}$$

and with $((c-a)(c+a)(c^2+a^2)(c^4+a^4)/2)$ remaining even, then $[((c-a)(c+a)(c^2+a^2)(c^4+a^4)/2)+a^8]$ is odd, and $[2\cdot((c-a)(c+a)(c^2+a^2)(c^4+a^4)/2+a^8)]$ is a product of the unique factor, 2^1.

And our result repeats for all n equal to a power of 2, ad infinitum; with each doubling of n resulting in only an increase of *one* in the count of the sums-of-powers terms of c and a, with a corresponding increase by *one* in the exponent of 2 in (c^n-a^n).

Let the notation, **[^2]** be read as "*the power of 2*". Let $(a,b,c) = (3,4,5)$.

Demonstration

$[\mathbf{^\wedge 2}] \in \boldsymbol{b^2 = [(2^2)^2 = 2^4]}$

$$\begin{aligned}(c^2-a^2) &= (5^2-3^2) = [(25-9) = 16] = 2^4 \\ &= (c-a)(c+a) = (2\cdot 8) = [(2^1\cdot 2^3) = 2^{(1+3)}] = \mathbf{2^4}\end{aligned}$$

$[\mathbf{^\wedge 2}] \in \boldsymbol{b^4 = (2^2)^4 = 2^8}$

$$\begin{aligned}(c^4-a^4) &= (5^4-3^4) = [(625-81) = 544] = (2^5\cdot 17) \\ &= (c^2-a^2)(c^2+a^2) = (c-a)(c+a)(c^2+a^2) \\ &= (2\cdot 8\cdot 34) = [(2^1\cdot 2^3)\cdot(2^1\cdot 17)] = (2^{(4+1)}\cdot 17) = (\mathbf{2^5}\cdot 17)\end{aligned}$$

$[\hat{}\mathbf{2}] \in \boldsymbol{b^8 = (2^2)^8 = 2^{16}}$

$$\begin{aligned}(c^8 - a^8) &= (5^8 - 3^8) = (390625 - 6561) = [384064 = (2^6 \cdot 6001)]\\ &= (c-a)(c+a)(c^2+a^2)(c^4+a^4)\\ &= (2 \cdot 8 \cdot 34 \cdot 706) = [(2^1 \cdot 2^3) \cdot (2^1 \cdot 17) \cdot (2^1 \cdot 353)]\\ &= [(2^{(4+1+1)} \cdot 17 \cdot 353) = (\mathbf{2^6} \cdot 6001)\end{aligned}$$

$[\hat{}\mathbf{2}] \in \boldsymbol{b^{16} = (2^2)^{16} = 2^{32}}$

$$\begin{aligned}(c^{16} - a^{16}) &= (5^{16} - 3^{16}) = (152587890625 - 43046721)\\ &= [152544843904 = (2^7 \cdot 1191756593)]\\ &= (c-a)(c+a)(c^2+a^2)(c^4+a^4)(c^8+a^8)\\ &= (2 \cdot 8 \cdot 34 \cdot 706) = [(2^1 \cdot 2^3) \cdot (2^1 \cdot 17) \cdot (2^1 \cdot 353) \cdot (2^1 \cdot 198593)]\\ &= [(2^{(4+1+1+1)} \cdot 17 \cdot 353 \cdot 198593) = (\mathbf{2^7} \cdot 1191756593)\end{aligned}$$

...

Then for all $n > 2$ equal to a power of 2, with the power of 2 in b^n equal to the power of 2 in b raised to the nth power; while the power of 2 in $(c^n - a^n)$ is equal to the power of 2 in $(c^2 - a^2) = b^2$, plus 1 for each sum of powers of c and a of exponents 2 to $n/2$; then the power of 2 in $(c^n - a^n)$ can never attain the value of the power of 2 in b^n; $(c^n - a^n)$ can never equal b^n, and $c = \sqrt[n]{(a^n + b^n)}$ can never be an integer. ■

Proposition 3.4 *Where $n > 2$ is equal to a power of 2 and $(c^n - b^n)$ is odd, $(c^n - b^n)$ can never equal a^n and $c = \sqrt[n]{(a^n + b^n)}$ can never be an integer*

Proof Let $(c^n - b^n)$ be the odd quantity of $(c^n - a^n)$ and $(c^n - b^n)$. With the reduction of $(c^n - b^n)$ proceeding in the exact same manner as that of $(c^n - a^n)$,

$$\begin{aligned}(c^{16} - b^{16}) &= [(c^8)^2 - (b^8)^2] \ = \ [(c^8 - b^8)(c^8 + b^8)]\\ &= [((c^4)^2 - (b^4)^2) \cdot (c^8 + b^8)] \ = \ [(c^4 - b^4)(c^4 + b^4)(c^8 + b^8)]\\ &= [((c^2)^2 - (b^2)^2) \cdot (c^4 + b^4)(c^8 + b^8)]\\ &= [(c^2 - b^2)(c^2 + b^2)(c^4 + b^4)(c^8 + b^8)]\\ &= [(c-b)(c+b) \cdot (c^2 + b^2)(c^4 + b^4)(c^8 + b^8)],\end{aligned}$$

then with $(c^2 - b^2) = (c-b)(c+b)$, and $(c+b) = ((c-b) + 2b)$;

and with the sum and difference of powers of c and b odd, and 2 and b both coprime to $(c-b)$, then $(c+b) = ((c-b)+2b)$ can contain no prime of $(c-b)$.

Similarly, $(c^2+b^2) = ((c^2-b^2)+2b^2)$, and with 2 and b^2 coprime to (c^2-b^2), then (c^2+b^2) can contain no prime of $(c^2-b^2) = (c-b)(c+b)$.

Likewise, $(c^4+b^4) = ((c^4-b^4)+2b^4)\ldots$ and (c^4+b^4) can contain no prime of $(c^4-b^4) = (c-b)(c+b)(c^2+b^2)$.

Continuing, $(c^8+b^8) = ((c^8-b^8)+2b^8)\ldots$ and (c^8+b^8) can contain no prime of $(c^8-b^8) = (c-b)(c+b)(c^2+b^2)(c^4+b^4)\ldots$

And for each successive increase in the power of 2 in n, $(c^{n/2}+b^{n/2}) = [(c^{n/2}-b^{n/2})+2b^{n/2}]$, and $(c^{n/2}+b^{n/2})$ can contain no prime of the reduced predecessor terms comprising $(c^{n/2}-b^{n/2})$; and for all $n > 2$ equal to a power of 2, the prime composition of each term of the sums and differences of powers of c and b in $(c^n - b^n)$ is coprime to all others.

Then where $(c^n - b^n)$ is odd and $n > 2$ is equal to a power of 2; with no prime of (c^2-b^2) in n or in $(c^2+b^2)(c^4+b^4)(c^8+b^8)\cdot\ \ldots\ \cdot(c^{n/2}+b^{n/2})$, then no power of any distinct prime in $(c^2 - b^2)$ within $(c^n - b^n)$ can ever be elevated beyond it's power at $n = 2$. Utilizing the Pythagorean triple, $(a, b, c) = (33, 56, 65)$ as an example:

Demonstration

$$\begin{aligned}
(c^2-b^2) &= 1089\\
&= (c-b)(c+b)\\
&= (65-56)(65+56) = (9\cdot 121) = (\mathbf{3^2}\cdot\mathbf{11^2})\\
&\Rightarrow\\
(c^4-b^4) &= 8016129\\
&= (c^2-b^2)(c^2+b^2)\\
&= (1089\cdot 7361)\\
&= [(\mathbf{3^2}\cdot\mathbf{11^2})\cdot(17\cdot 433)]\\
(c^8-b^8) &= 221927501316609\\
&= [(c^2-b^2)(c^2+b^2)(c^4+b^4)]\\
&= (1089\cdot 7361\cdot 27685121)\\
&= [(\mathbf{3^2}\cdot\mathbf{11^2})\cdot(17\cdot 433)\cdot 27685121]\\
(c^{16}-b^{16}) &= 92180278423996126856766522369\\
&= [(c^2-b^2)(c^2+b^2)(c^4+b^4)(c^8+b^8)]\\
&= (1089\cdot 7361\cdot 27685121\cdot 415362124464641)\\
&= [(\mathbf{3^2}\cdot\mathbf{11^2})\cdot(17\cdot 433)\cdot 27685121\cdot 415362124464641].
\end{aligned}$$

And for all $n > 2$ equal to a power of 2, with $(c^n - b^n)$ always a product of the distinct and unique primes in $(c^2 - b^2) = a^2$, and no power of any distinct prime in $(c^2 - b^2)$ greater than the square of its power in a; while the power of each distinct prime in a^n is equal to its power in a raised to the nth power, then $(c^n - b^n)$ can never equal a^n and $c = \sqrt[n]{(a^n + b^n)}$ can never be an integer. ■

References

[1] Aczel, Amir D. Fermat's Last Theorem. *Dell Publishing, New York*, 1996. 44.

[2] Dolciani, Mary P.; Wooton, W; Beckenbach, E. F.; Sharron, S.. Modern School Mathematics - Algebra and Trigonometry 2. *Houghton Mifflin Company, Boston*, 1971. 317.

[3] Fuller, Gordon. College Algebra. Third Edition. *Van Nostrand Reinhold Company, New York*, 1969. 20-21.

[4] Goldstein, Larry Joel. Algebra and Trigonometry and Their Applications. *Richard D. Irwin, Boston*, 1993. 550.

[5] Gregerson, Erik. Editor. The Britannica Guide To The History of Mathematics. PDF. *Britannica Educational Publishing, New York*, 2011. 77; 139.

[6] Koshy, Thomas. Elementary Number Theory with Applications. *Harcourt / Academic Press, Burlington MA*, 2002. 546.

[7] Nagell, Trygve. Introduction To Number Theory. PDF. *John Wiley and Sons, New York -and- Almqvist and Wiksell, Stockholm*, 1951. 252.

[8] Ribenboim, Paulo. 13 Lectures on Fermat's Last Theorem. *Springer-Verlag New York Inc.*, 1979. 2-3

[9] Weisstein, Eric W.. Fermat's Last Theorem—*From MathWorld, A Wolfram Web Resource*, January 5, 2006. `http://mathworld.wolfram.com/FermatsLastTheorem.html`. Last accessed, September 22, 2017.

Post Office Box 342, Chapel Hill NC 27514, U.S.A.